

Unternehmenswerte schützen – Wertschöpfung sicherstellen

Das war der VZP-Tag 2022 im Hotel Hilton Frankfurt Airport

12. Mai 2022

Vorträge | Expertenrunden | Get-together

Premiere beim VZP-Tag: Zum ersten Mal konnten sich Teilnehmende im hybriden Format austauschen. Zwei spannende Podiumsdiskussionen zu aktuellen Themen aus Risikomanagement, Versicherungsmarkt, Sachwert-Sicherung und Cybersicherheit wurden vor Ort geführt und per Live-Stream übertragen.

Unter der Moderation von Dr. Kristina Klinkforth, Leiterin der Funk Akademie, und Horst Ullrich, Geschäftsführer VZP, wurde angeregt diskutiert: Wie lassen sich Unternehmenswerte in anspruchsvollen Zeiten schützen? Was macht Unternehmen der Papierwirtschaft attraktiv für Versicherer? Und welche Maßnahmen können Unternehmen ergreifen, um zunehmende Cyberangriffe abzuwehren?

Am Ende eines Tages mit Networking und Diskussionen stand ein zentraler Gedanke: Nicht vor den Herausforderungen kapitulieren, sondern gemeinsam neue Lösungen schaffen.

Die Expertenrunden in der Zusammenfassung



Expertenrunde 1 | Industriesachversicherung im Wandel – Unternehmenswerte schützen

Nigel Todd | Vice President FM Global

Dr. Alexander Skorna | GF Funk Risk Consulting

Dr. Jan Klingele | GS/GF Klingele Papierwerke GmbH & Co. KG

Frank Gumbinger | CFO Papierfabrik Adolf Jass GmbH & Co. KG

- › **Vortrag:** Dr. Jan Klingele, geschäftsführender Gesellschafter der Klingele Gruppe: „Wie werde ich attraktiv für meinen Versicherer?“
- › **Kernaussagen des Vortrags:** Für Industrieunternehmen wird es schwieriger, für die Versicherer so attraktiv zu sein, dass sie zu günstigen Bedingungen adäquaten Versicherungsschutz erhalten. Selbst wer bisher hochattraktiv war, kann diesen Status blitzschnell durch externe Faktoren verlieren, die außerhalb der eigenen Einflussphäre liegen. Durch Verbesserungen der Prozesse zur Schadenvermeidung und -minimierung sowie Investitionen in Schutzvorrichtungen lassen sich (noch immer) die Chancen für einen guten Versicherungsschutz erhöhen. Aber andere Faktoren wie die Größe des Versicherungsnehmers, die Nähe zum Versicherer, die Wahl der Länder für seine Standorte, die Gefährdung durch Naturgefahren und die Art seiner Aktivitäten scheinen wichtiger zu werden.
- › **Diskussion:** Trotz Investitionen in Brandschutzprävention gab es in den letzten Jahren deutliche Prämien erhöhungen. Die Selbstbehalte werden größer, Vertragslaufzeiten kürzer.
- › In der Folge entsteht akuter Handlungsbedarf. Ein Lösungsansatz hierfür ist permanentes Risikomanagement mit den Kernfragen: Wie wird das eigene Risiko bewertet? Welche Schutzmaßnahmen können Risiken reduzieren?
- › Generell ist es Zeit, umzudenken und konventionelle Ansätze zu hinterfragen. So kann Schadenprävention etwa durch Digitalisierung sowie den Einsatz von Sensorik erfolgen.
- › Wichtig ist es, dass Versicherer und Versicherungsnehmer angesichts der immer vielschichtigeren Risikolandschaft Hand in Hand gehen.
- › Obwohl Prämien und Selbstbehalte in den letzten Jahren gestiegen sind, lohnt es sich trotzdem, in die Risikoverbesserung bzw. den Brandschutz zu investieren. Dadurch werden Prämien so stabil wie möglich gehalten und gleichzeitig die Resilienz der Standorte deutlich erhöht.
- › Die Papierwirtschaft könnte mehr Stärke durch Gemeinschaft herstellen. Wäre es eine Option, traditionelle Deckungen zu kappen und alternativen Versicherungsschutz (z. B. parametrische Versicherungen) zu nutzen? Denn auch weniger gut geschützte Risiken müssen abgesichert werden: Wechselwirkungsschäden und Business Continuity Management sind für Versicherungsnehmer herausfordernd. Eine Sensibilität gegenüber dieser Problemstellung seitens der Versicherer wäre wünschenswert.
- › **Schlussappell:** Trotz der Herausforderungen auf dem verhärteten Markt ist es bedeutsam, nicht zu resignieren und Prämienstabilität anzustreben.

„Werden Sie intrinsisch aktiv, um Ihre Unternehmenswerte zu schützen. Die VZP begleitet Sie bei alternativen Finanzierungen und Risikolösungen.“

Thomas Abel, Geschäftsführer VZP





Expertenrunde 2 | Bedrohungsszenario Cyberangriff – Wertschöpfung sicherstellen

Andreas Pankow | CEO Deutsche Gesellschaft für Cybersicherheit mbH & Co. KG

Alexandra Köttgen | Cyber Claims Expertin Funk Hamburg

Sven Gohmann | Cyber Security Consultant Funk Hamburg

- › Die **Cyberbedrohung** ist omnipräsent, alle 39 Sekunden wird in Deutschland ein Cyberangriff erfolgreich durchgeführt.
- › Ein Cyberangriff erfolgt schleichend: Es können 3 bis 6 Monate vergehen, bis ein erfolgter Angriff sich bemerkbar macht. Die Schäden sind enorm. Im Durchschnitt werden Unternehmen z. B. durch Verschlüsselung 3 bis 6 Monate lahmgelegt, bis die operativen Funktionen weitestgehend wiederhergestellt sind.
- › **Cyberschutz wird daher immer bedeutender für Unternehmen.** Konzerne sind von Cyberkriminalität genauso betroffen wie kleine und mittelständische Unternehmen.
- › Ein Rat an Unternehmen: Cybersicherheit sollte nicht nur in der IT angesiedelt sein, sondern muss von der Unternehmensführung über alle Bereiche hinweg implementiert werden. Die Gefahren-Sensibilisierung von Mitarbeitenden ist dabei ein zentraler Bestandteil.
- › Eine professionelle Analyse der Bedrohungslage (Penetrationstest) ist ein starkes Mittel zur Prävention. Der Test deckt potenzielle Schwachstellen auf. Elementar ist auch eine kontinuierliche Überwachung des gesamten digitalen Ökosystems. Dabei unterstützen kann externe Cyberexpertise, die zugleich eine Überforderung der Inhouse-IT vermeidet.
- › In der Papierwirtschaft ergibt sich aus der langen Laufzeit der Produktionsmaschinen eine erhöhte Cybergefährdung, denn die Hersteller sind meist für die Aktualität der damit verbundenen IT-Systeme verantwortlich. Updates zur Verbesserung der Sicherheit erfolgen mit verstrichener Zeit seltener. Um mögliche Gegenmaßnahmen ergreifen zu können, ist es für die Unternehmen wichtig, eine Übersicht der verwendeten IT-Infrastruktur zu haben, um gezielt handeln zu können.
- › **Welche Auswirkungen hat die gestiegene Cybergefahr auf den Versicherungsschutz von Unternehmen?**
Die Anforderungen der Versicherer an technische und organisatorische IT-Sicherheitsmaßnahmen sind drastisch gestiegen. Gleichzeitig wächst der Absicherungsbedarf bei Unternehmen mit zunehmender Bedrohung, auch bedingt durch die mediale Präsenz des Themas. Das Sicherheitsniveau vieler Unternehmen weist dabei derzeit teils gravierende Lücken zu den Erwartungen der Versicherer auf.
- › Die VZP begleitet Sie bei der Risikoaufnahme und berät zu ggf. erforderlichen Maßnahmen, die für den Einkauf von Versicherungsschutz erforderlich sind. Das erstellte Risikoprofil bildet die Basis für den anschließenden Dialog mit den Versicherern.
- › **Im Fall einer Cyberattacke** ist es wichtig, schnell und zielgerichtet zu agieren. Auch beim bloßen Verdacht auf einen Cyberschaden sollte der Versicherer informiert werden. Professionelle IT-Hilfe sollte zur Unterstützung hinzugezogen werden. Zu beachten ist, dass offizielle Meldungen an Behörden innerhalb der ersten 72 Stunden nach Kenntnis eines Datenschutzvorfalls mithilfe eines Formulars abzusetzen sind.
- › Versicherungsschutz stellt lediglich eine Säule für Cyberschutz dar. Die **Eigeninitiative der Unternehmen ist maßgeblich gefragt**, um sich effizient gegen Cyberangriffe abzusichern.

„Anspruchsvolle Zeiten verlangen, dass wir künftig noch intelligenter agieren und unsere Stärke als Gemeinschaft der Papierwirtschaft einsetzen.“

Horst Ullrich, Geschäftsführer VZP

Impressionen

